Qualys Container Security

Release Notes

Version 1.10
May 12, 2021 (Updated June 3, 2021)

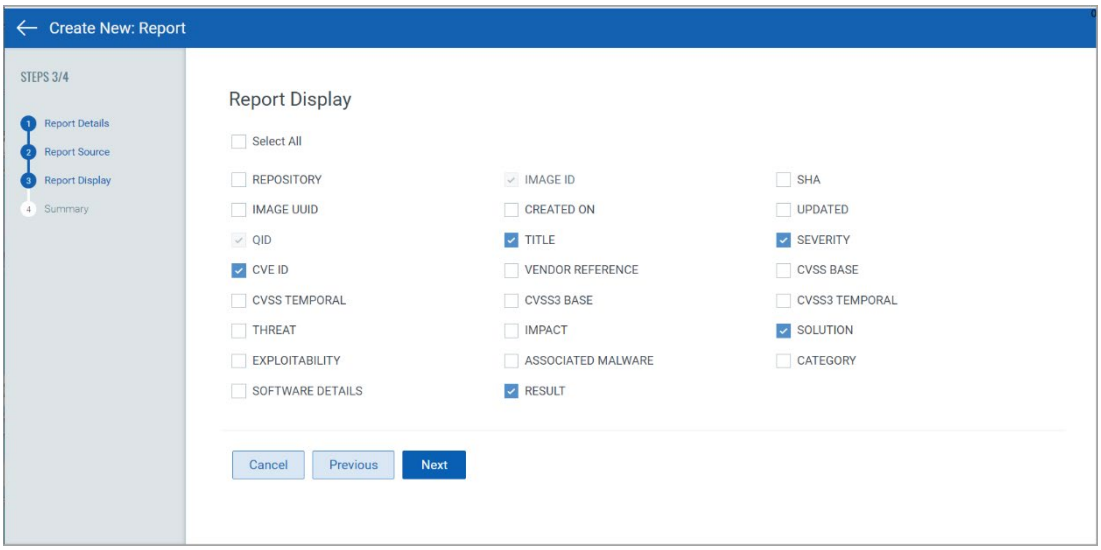
Here's what's new in Container Security 1.10!

Container Security 1.10 brings you more improvements and updates! Learn more

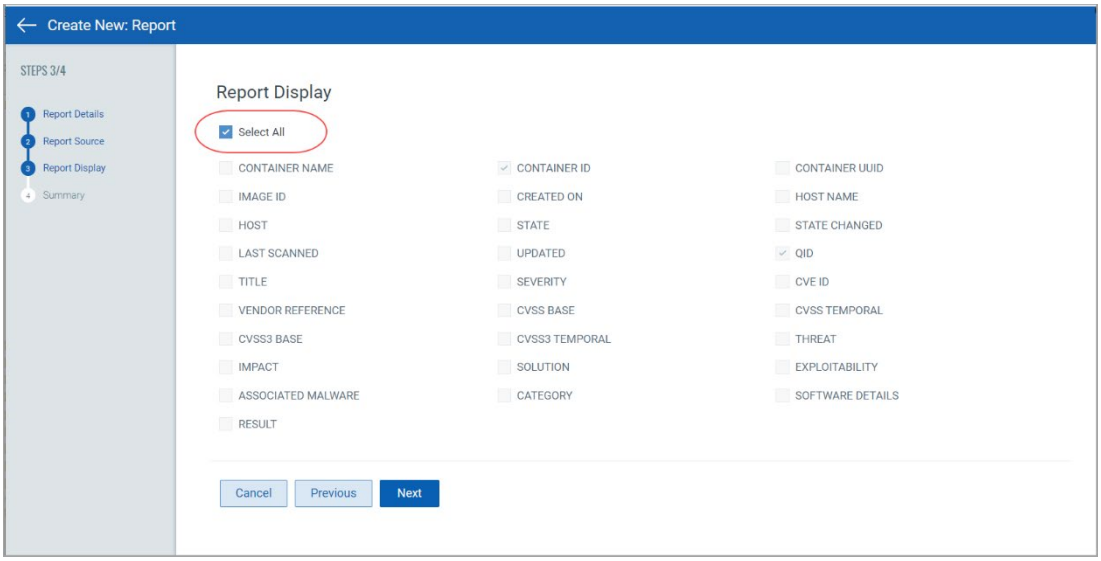
Now You Can Customize Vulnerability Report Details

Prior to this release, all report details were included in Image and Container Vulnerability Reports and this was not something you could customize. Now, while creating a new report, you get to choose which image/container and vulnerability details to display in the report. Simply select the check box next to each detail you want to include in the report. Your selections determine which columns appear in the CSV report output. Note that certain details are selected by default and cannot be unchecked. Want to include all details? Pick the "Select All" option and all details will be included.

In this example, we're creating a new Image Vulnerability Report. The following details will be included in the report: QID, Image ID, CVE ID, Title, Result, Severity and Solution.



In this example, we're creating a new Container Vulnerability Report. All details will be included in the report because the "Select All" option is checked.



Collection of Kubernetes Cluster Attributes

In this release we have added collection of Kubernetes cluster attributes and made this information searchable in the UI. Kubernetes cluster attributes include node details, pod details (name, uuid, namespace, labels), controller details (name, uuid, type) and more. Use Container Security APIs to see the Kubernetes cluster attributes collected for your containers and sensors.

Important - Kubernetes attributes will only be processed for containers discovered after the version 1.10 release. Kubernetes attributes are collected as part of container inspect processing when containers are discovered for the first time. To fetch Kubernetes cluster attributes for an existing deployment in Kubernetes, you will have to "rollout restart" the existing deployment, which will create new containers and this will start the container inspect processing. Kubernetes attributes will get collected for the newly created containers on Kubernetes clusters.

Use the following command for the "rollout restart":

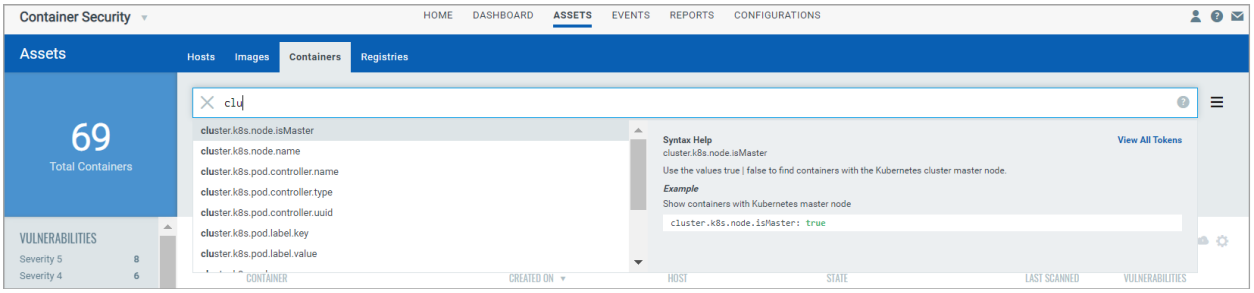
```
kubectl rollout restart deployment <deployment-name> -n <namespace>
```

Kubernetes cluster attributes:

- Cluster type (Kubernetes)
- Cluster version
- Project name (collected for projects in Google Cloud Platform)
- Node name and flag indicating whether the node is the master node
- Pod name
- Pod UUID
- Pod namespace
- Pod labels (key and value pairs)
- Controller name
- Controller UUID
- Controller type (e.g. DaemonSet, Deployment, ReplicaSet, etc)

New Search Tokens for Kubernetes Cluster Attributes

Now you can search the Kubernetes cluster attributes collected by the sensor. Use new search tokens starting with cluster.k8s when searching containers (under **Assets** > **Containers**) or sensors (under **Configurations** > **Sensors**).



The table below describes new search tokens. See the syntax help in the UI for more details.

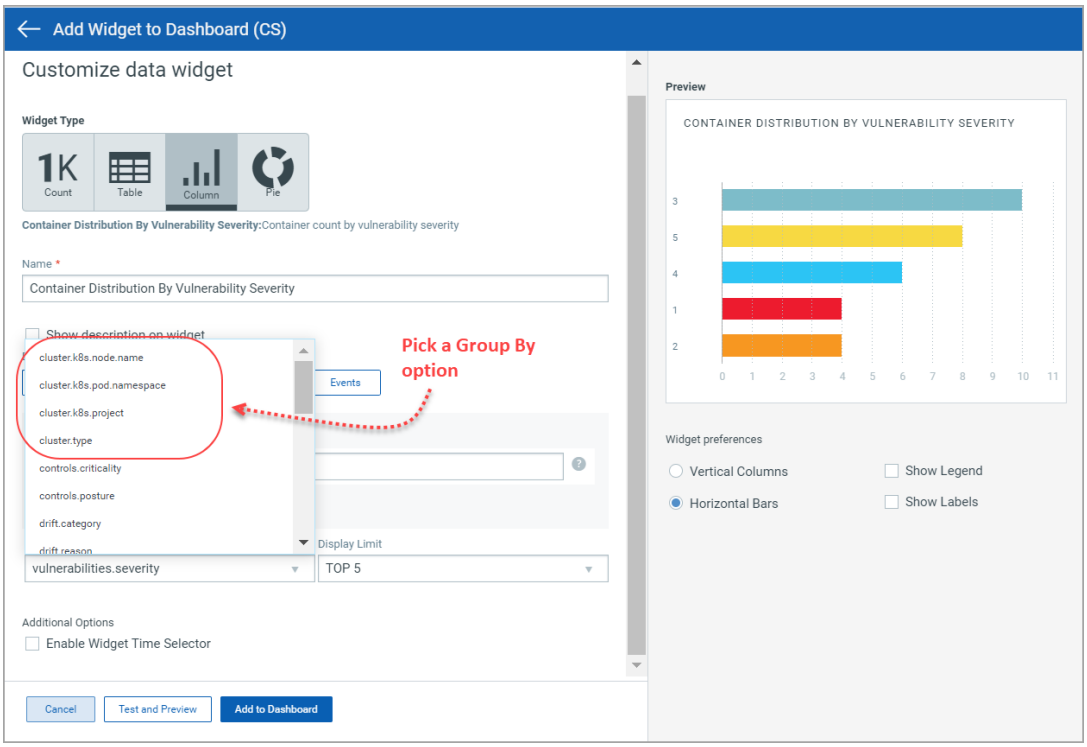
Token	Description
cluster.k8s.node.isMaster	Find containers/sensors running on the master node.
cluster.k8s.node.name	Search by the name of the node that the pod is assigned to.
cluster.k8s.pod.controller.name	Search by the name of the controller that the pod belongs to.
cluster.k8s.pod.controller.type	Search by the controller type. When searching containers, possible values are CronJob, DaemonSet, Deployment, Job, Node, ReplicaSet, ReplicationController, StatefulSet. When searching sensors, only DaemonSet is valid.
cluster.k8s.pod.controller.uuid	Search by the controller UUID.
cluster.k8s.pod.label.key	Search by a label name (key) assigned to the pod.
cluster.k8s.pod.label.value	Search by a label value assigned to the pod.
cluster.k8s.pod.name	Search by the pod name.
cluster.k8s.pod.namespace	Search by the name of the namespace where the pod is running.
cluster.k8s.pod.uuid	Search by the pod UUID.
cluster.k8s.pod.project	Search by the project name.
cluster.type	Search by the cluster type. Only KUBERNETES is valid.

New Group By Options for Kubernetes Cluster Attributes

When creating a widget for your Container Security dashboard, you'll see new Group By options for Kubernetes cluster attributes. Use Group By options for widget types Table, Column and Pie.

When you display results by Container or Sensor, you'll see these new Group By options:

- cluster.k8s.node.name
- cluster.k8s.pod.namespace
- cluster.k8s.project
- cluster.type



Downloading and Deploying the Container Sensor is Easier Than Ever!

We made several improvements to the Download Sensor workflow to make downloading and deploying the sensor easier than ever.

You'll notice these changes in the UI:

- Step-by-step installation instructions are available in the UI for deploying the sensor on supported standalone technologies (MacOS, Linux, CoreOS) and for cluster environments (Docker Swarm, Kubernetes, Openshift, DCOS, AWS ECS).

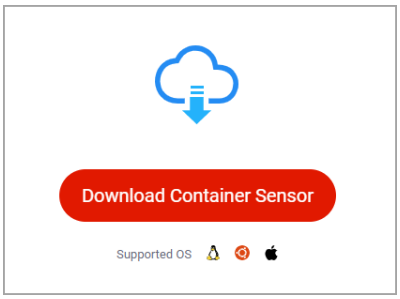
- For standalone installations, you can choose whether you want to see instructions for installing the sensor using the provided tar file or installing the sensor from Docker Hub.

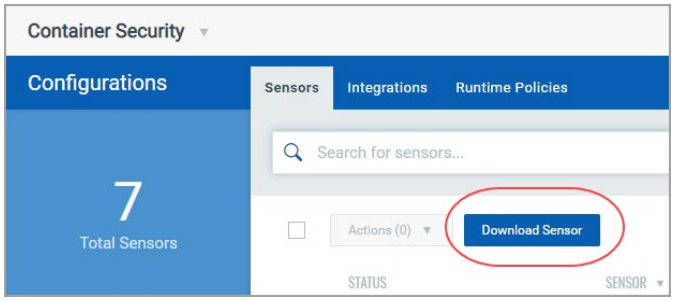
- For cluster installations, you can view instructions for different runtimes (Docker Runtime, Containerd Runtime and CRI-O Runtime), when applicable.

- Installation yaml files for certain deployments can now be downloaded directly from the UI and are pre-filled with your activation ID, customer ID and POD URL. Previously users had to extract yaml files from the tar and manually customize them.

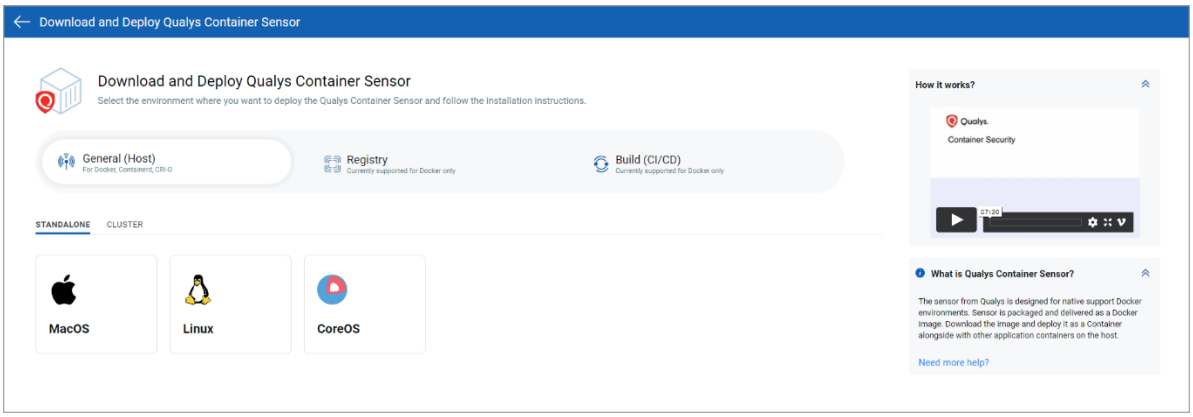
What are the steps?

To get started, either click the **Download Container Sensor** button on the **Home** page, or go to **Configurations** > **Sensors** and click **Download Sensor**.

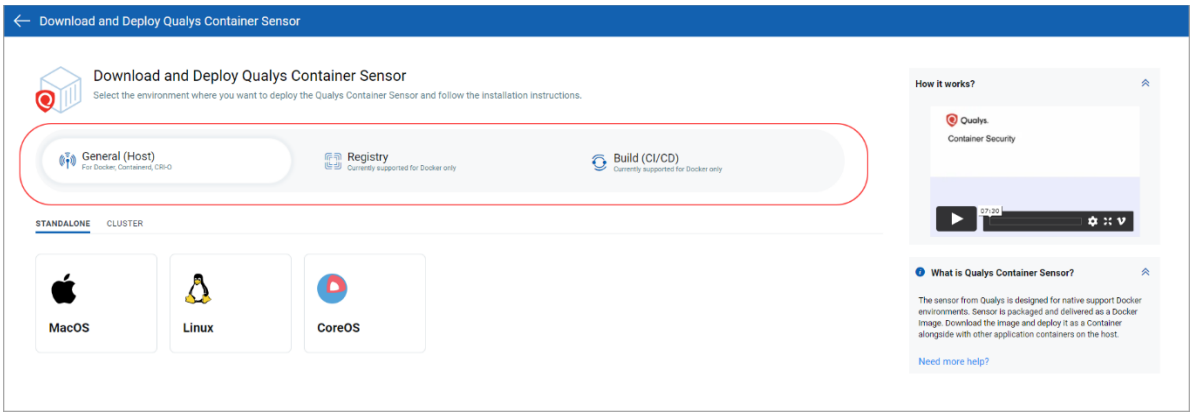




The **Download and Deploy Qualys Container Sensor** window will appear, as shown below.

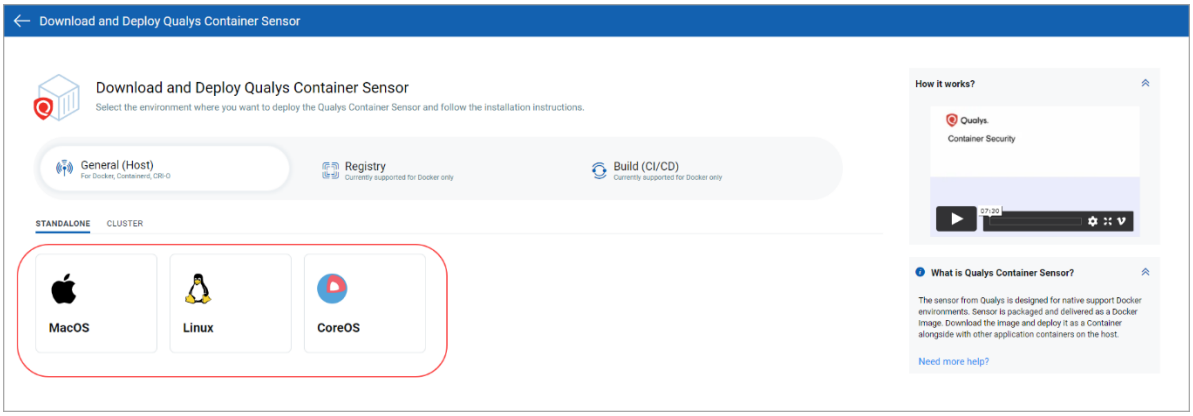


Pick the type of sensor you want to deploy – General (Host), Registry or Build (CI/CD).

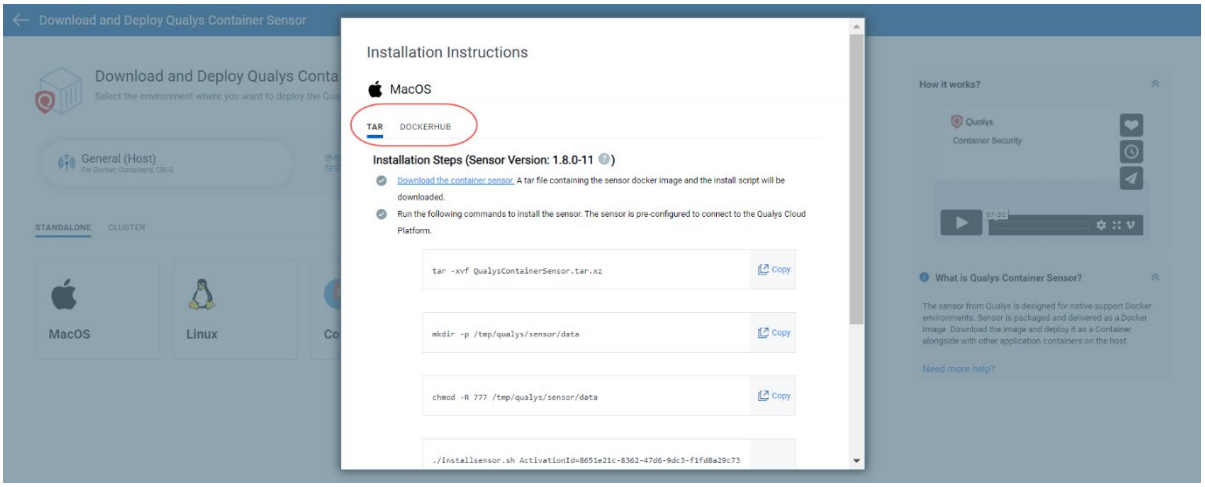


For a standalone deployment:

To deploy on a standalone host, pick the host's operating system: MacOS, Linux or CoreOS.

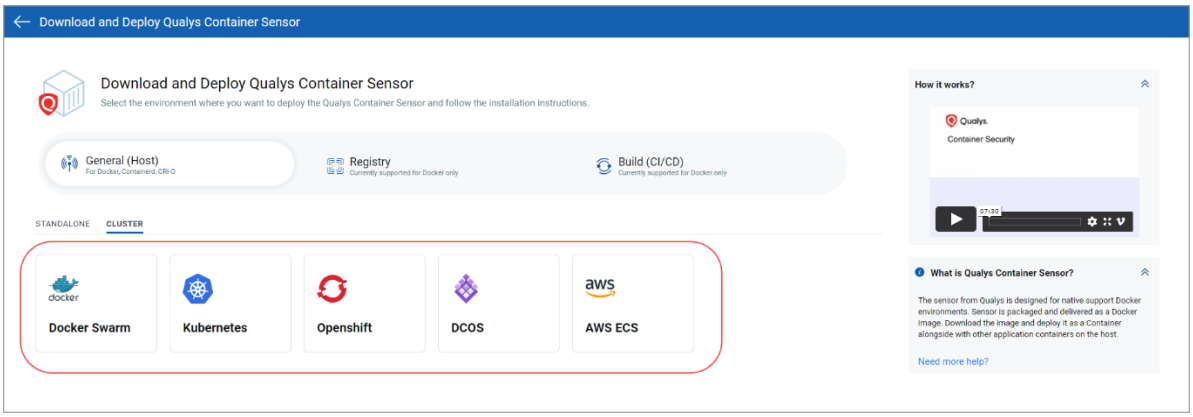


In the window that appears, choose **TAR** or **DOCKERHUB** for how you want to install the sensor. Simply follow the steps on the screen. For Tar, you'll download the tar file and run the install commands on the screen. For Docker Hub, you'll run the docker commands on the screen.

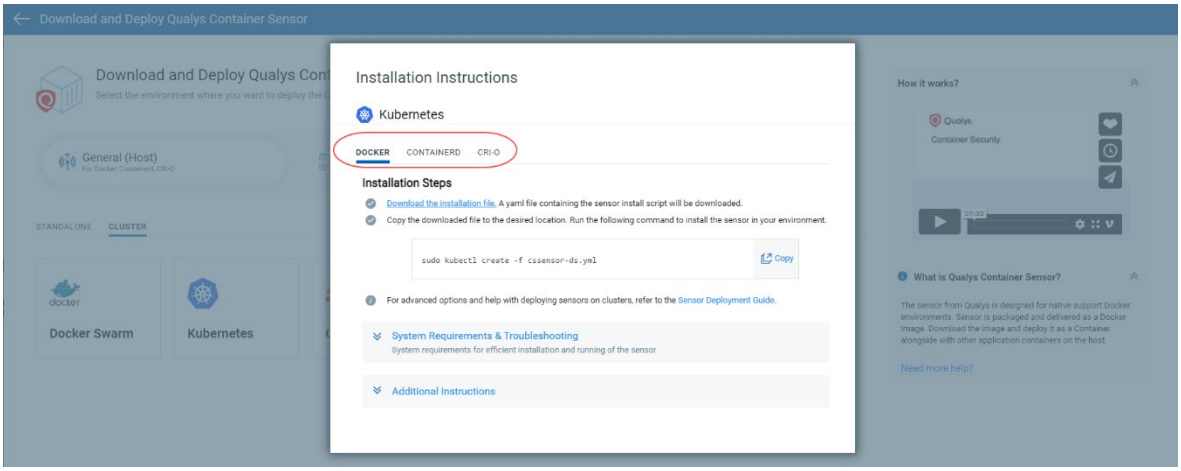


For a cluster deployment:

To deploy to a cluster, first pick the cloud environment: Docker Swarm, Kubernetes, Openshift, DCOS or AWS ECS.

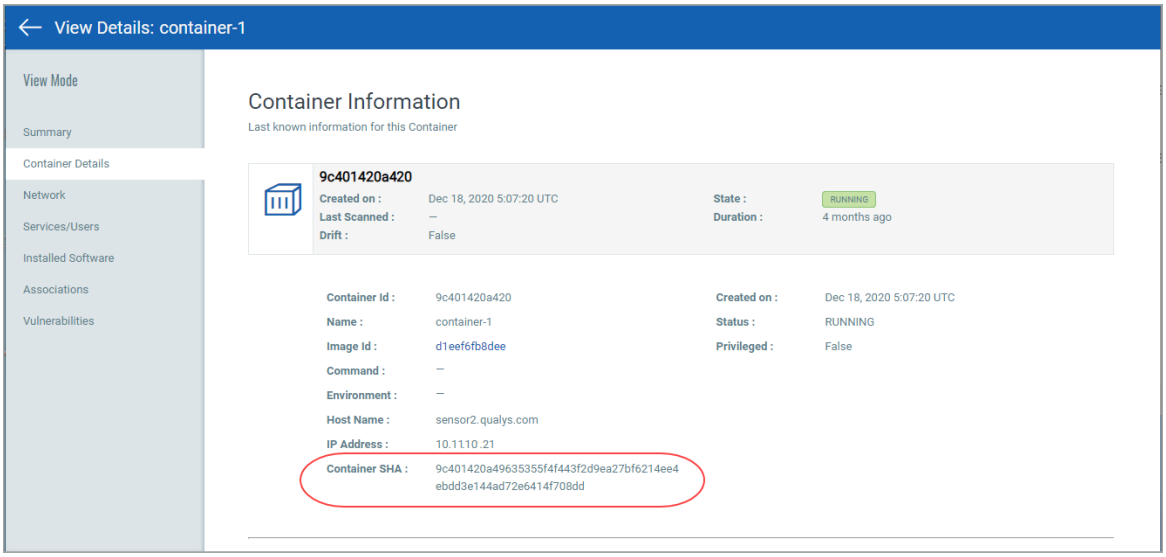


In the window that appears, choose the runtime. In the example below for General sensor being deployed in Kubernetes, you'll see **DOCKER**, **CONTAINERD** and **CRI-O** runtime options. After making your selection, simply follow the steps on the screen. The installation yaml file that you download will already be pre-filled with your activation ID, customer ID and POD URL.



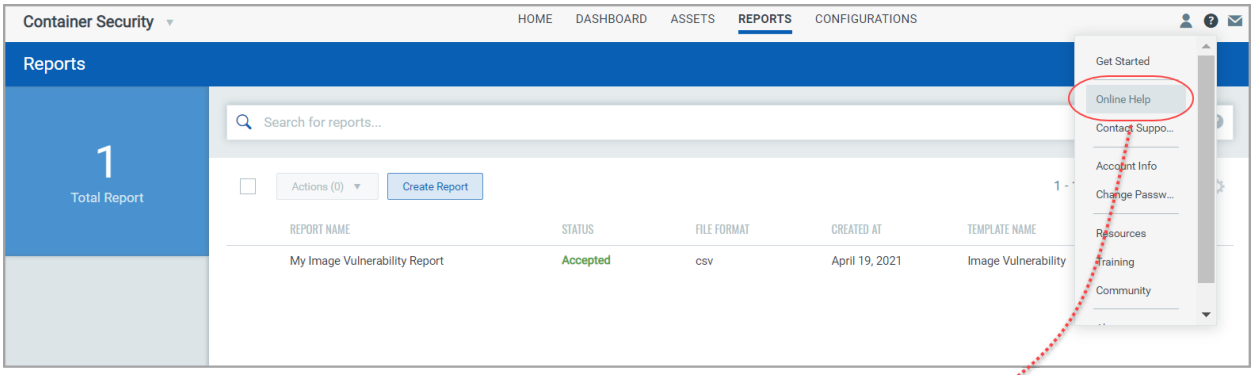
Container SHA Value Now Appears in Container Details

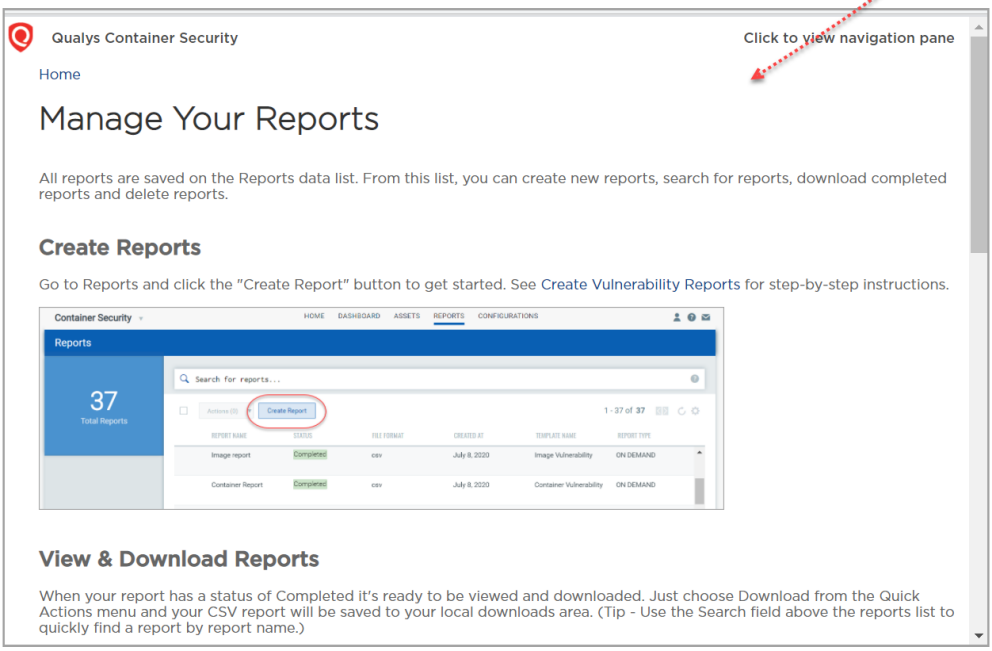
The Container SHA value is required for several Container Runtime Security (CRS) APIs. We added this value to the UI so you can more easily find it. Just go to the **Assets** > **Containers** list and choose **View Details** for any container listed. The SHA value will appear on the **Container Details** tab.



Online Help Improvement

Starting with this release, when you choose the Online Help option you'll get help that is relevant to where you are in the Container Security UI. For example, if you're in the Reports section of the UI and you choose Online Help, you'll get help for Reports. If you're in the Assets section of the UI and you choose Online Help, you'll get help for Assets, and so on. Once in the help, the navigation pane and Search options are available to assist you further.





Issues Addressed

- Fixed a report download issue where large reports were failing to download.
- Fixed the search for host associations inside image and container details. Now the correct search tokens are listed in the search bar.
- Fixed an issue where GCP and ACR registry API endpoints were missing for v1.2 and v1.3 in the gateway swagger UI.
- Fixed an issue where event details for instrumented containers incorrectly showed text in the UI that the process was “communicating with null”.